IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

SECURITY FIRST INNOVATIONS, LLC, Plaintiff, v. GOOGLE LLC, Defendant.	Case No. 2:23-cv-97

MEMORANDUM OPINION & ORDER

Before the Court are two motions: Plaintiff Security First Innovations, LLC's ("SFI's") Motion for Leave to Amend its Complaint (ECF No. 73) and Defendant Google LLC's ("Google's") Motion to Dismiss the Complaint (ECF No. 37). In the interests of efficiency and judicial economy, the Court will address both motions in this Memorandum Opinion and Order. The Court has fully considered the arguments set forth in the parties' briefs and has determined it is not necessary to hold a hearing on the motions. For the reasons stated below, SFI's motion to amend is **GRANTED** and Google's motion to dismiss is **DENIED.**[1]

[1] On October 25, 2023, the parties filed a stipulation indicating their agreement that "[w]hether the Court grants or denies SFI's Motion for Leave, Google does not need to re-file or re-brief its Motion to Dismiss because SFI's Proposed Amended Complaint does not affect the arguments made in support of or in opposition to Google's Motion to Dismiss." ECF No. 122 at 2. The parties further agreed that the motion to dismiss "shall apply to both the Proposed Amended Complaint and the Complaint, and can be decided by the Court as currently briefed subject to the parties' request for oral argument." *Id.* Accordingly, because the Court grants SFI's motion for leave to

I. BACKGROUND

A. The Asserted Patents

The four asserted patents are U.S. Patent Nos. 10,452,854 ("the '854 patent"), 11,068,609 ("the '609 patent"), 11,178,116 ("the '116 patent"), and 9,338,140 ("the '140 patent"). The '609 patent is a continuation of the '854 patent, and the '116 patent is a continuation of a continuation of the '140 patent.

SFI asserts claim 1 of each asserted patent against Google. The asserted claims are all fairly similar.[2] At a high level, the claims are directed to a method for securing data that involves splitting data, encrypting the data with encryption keys, and storing the data and the encryption keys in one or more places. Claim 1 of the '609 patent, which the parties focus on in the briefing, is below:[3]

> A method for securing data, the method comprising:

---

amend, the Court construes Google's motion to dismiss to be directed to the amended complaint.

[2] This statement should not be taken as a finding of representativeness. There are differences between the claims that are relevant to the Court's analysis of the § 101 issues raised in Google's motion, as discussed below.

[3] SFI argues in its opposition that Google has largely ignored all but the '609 patent in its motion to dismiss, such that the Court should treat the motion as only being directed to the '609 patent. ECF No. 42 at 35. That is not correct. Google addresses the differences between the asserted claims several times in its motion. *See* ECF No. 38 at 16–17, 22, 24–25, 28–29, 31. In any event, "[a]ddressing each asserted claim in a § 101 analysis is unnecessary when the claims are 'substantially similar and linked to the same abstract idea.'" *Pers. Beasties Grp. LLC v. Nike, Inc.*, 341 F. Supp. 3d 382, 386 (S.D.N.Y. 2018) (quoting *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n*, 776 F.3d 1343, 1348 (Fed. Cir. 2014)). In this case, while there are some differences between the claims that play a role in some parts of the Court's § 101 analysis, the claims can largely be treated together because they are substantially similar.

> executing code by a processor to perform:
>
> > receiving a first key from a storage system;
> >
> > generating a plurality of data chunks based on a data set, wherein each data chunk of the plurality of data chunks comprises less than an entirety of data of the data set, and wherein the data set can be reconstructed using at least a minimum number of the plurality of chunks;
> >
> > encrypting each respective data chunk of the plurality of data chunks with a respective second key, wherein each of the respective second keys are distinct from each other;
> >
> > performing a cryptographic operation based on the first key to further secure the plurality of data chunks; and
> >
> > storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one storage device.

'609 patent, 83:11–30. Claim 1 of the '854 patent, which is the parent of the '609 patent, claims the following:

> A method for securely storing a data set, the method comprising:
>
> receiving an external key from an external storage system,
>
> generating a plurality of data chunks based on the data set,
>
> > such that the data set can be reconstructed using at least a minimum number of the plurality of data chunks, wherein generating the data chunks comprises:
> >
> > distributing the data set into a plurality of shares, wherein each of the shares comprises less than all of the data set,

> accessing a plurality of distinct encryption keys,
>
> encrypting each of the shares with a respective one of the plurality of distinct encryption keys,
>
> performing an encryption operation based on the external key to further secure the plurality of data chunks; and
>
> storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys on a plurality of different storage devices.

'854 patent at 83:19–36. Claim 1 of the '140 patent claims the following:

> A secure storage network comprising:
>
> a plurality of physical storage devices storing thereon a plurality of shares being associated with at least one session key used to secure a dataset; and
>
> a secure storage system configured to:
>
> present to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device;
>
> generate the plurality of shares for storage on the plurality of physical storage devices by performing a securing operation on the dataset received from the client device and distributing the dataset in the shares;
>
> include with each of the plurality of shares data indicative of the at least one session key used to secure the dataset; and
>
> reconstitute the dataset from at least a portion of the plurality of shares stored on the physical storage devices in response to a request from the client device for information in the dataset.

'140 patent, 98:2–22. Claim 1 of the '116 patent, which is a grandchild of the '140 patent, claims the following:

> A method for securing a data set, the method comprising:
>
> distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;
>
> encrypting each of the data chunks with a respective one of a plurality of encryption keys;
>
> obfuscating each of the plurality of different encryption keys; and
>
> separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices.

'116 patent, 100:19–31.

B. Procedural History

SFI filed the complaint in this case on March 10, 2023. ECF No. 1. The complaint alleged that the Google Cloud service infringes the four asserted patents. Google filed the instant motion to dismiss on April 28, 2023. ECF Nos. 37 (motion), 38 (memorandum). SFI filed an opposition on May 19, 2023. ECF No. 42. Google filed a reply on June 1, 2023. ECF No. 43. Each party filed a notice of supplemental authority on September 20, 2023, ECF Nos. 99 (Google), 109 (SFI).

SFI filed the instant motion for leave to amend the complaint on August 21, 2023. ECF Nos. 73 (motion), 74 (memorandum). Google filed a brief in opposition on September 8, 2023. ECF No. 88. SFI filed a reply on September 14, 2023. ECF No. 93. SFI filed a "Notice of Supplemental Information Regarding Google's Knowledge

of the Asserted Patents" on September 20, 2023. ECF No. 101. Google filed a response to SFI's notice, with leave, on October 12, 2023. ECF No. 118.

The parties are currently engaged in discovery, and a jury trial is set for July 9, 2024. ECF No. 54.

II. LEGAL STANDARDS

A. Motions to Amend a Complaint

Fed. R. Civ. P. 15(a) provides that a party may amend a pleading by leave of the court or by written consent of the adverse party, and that "[t]he court should freely give leave [to amend] when justice so requires." Leave to amend "should be denied only when the amendment would be prejudicial to the opposing party, there has been bad faith on the part of the moving party, or the amendment would [be] futile." *Laber v. Harvey*, 438 F.3d 404, 426 (4th Cir. 2006) (quotation marks and citation omitted). A proposed amendment is futile if the new claim would not survive a motion to dismiss under Fed. R. Civ. P. 12(b)(6). *Davison v. Randall*, 912 F.3d 666, 690 (4th Cir. 2019).

B. Willful Infringement

Under 35 U.S.C. § 284, a court may increase a damages award for patent infringement by "up to three times the amount found or assessed." Section 284 "prescribes no standards for such increase," *SRI Int'l, Inc. v. Advanced Tech. Lab'ys, Inc.*, 127 F.3d 1462, 1464 (Fed. Cir. 1997), but it has long been recognized as providing for "punitive or increased damages . . . in a case of willful or bad-faith infringement."

Halo Elecs., Inc. v. Pulse Elecs., Inc., 579 U.S. 93, 100 (2016) (quoting *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 377 U.S. 476, 508 (1964)) (cleaned up).

The Supreme Court has "eschew[ed] any rigid formula for awarding enhanced damages under § 284," noting that "[d]istrict courts enjoy discretion in deciding whether to award enhanced damages, and in what amount." *Halo*, 579 U.S. at 104. Enhanced damages "should generally be reserved for egregious cases typified by willful misconduct" that go "beyond typical infringement." *Id.* at 106, 110. "The subjective willfulness of a patent infringer, intentional or knowing, may warrant enhanced damages." *Id.* at 105. But "it is the circumstances that transform simple 'intentional or knowing' infringement into egregious, sanctionable behavior." *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1308 (Fed. Cir. 2019) (quoting *Halo*, 579 U.S. at 111 (Breyer, J., concurring)) (emphasis removed).

Courts have held that "a willful infringement-based claim for enhanced damages survives a motion to dismiss if it alleges facts from which it can be plausibly inferred that the party accused of infringement (1) had knowledge of or was willfully blind to the existence of the asserted patent and (2) had knowledge of or was willfully blind to the fact that the party's alleged conduct constituted, induced, or contributed to infringement of the asserted patent." *Dynamic Data Techs., LLC v. Amlogic Holdings Ltd.*, No. 1:19-cv-1239, 2020 WL 4365809, at *5 (D. Del. July 30, 2020); *see also, e.g.*, *Malvern Panalytical Ltd v. Ta Instruments-Waters LLC*, No. 1:19-cv-2157, 2021 WL 3856145, at *2 (D. Del. Aug. 27, 2021).

C. Motions to Dismiss

"To survive a [Rule 12(b)(6)] motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). In other words, a plaintiff must plead sufficient "factual content [that] allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "Factual allegations must be enough to raise a right to relief above the speculative level on the assumption that all of the complaint's allegations are true." *Twombly*, 550 U.S. at 545. When considering a motion to dismiss, the court "must take all the factual allegations in the complaint as true," but the court is "not bound to accept as true a legal conclusion couched as a factual allegation." *Papasan v. Allain*, 478 U.S. 265, 286 (1986).

D. Abstractness Under § 101 of the Patent Act

"Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." 35 U.S.C. § 101. The Supreme Court has "long held that this provision contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable." *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013) (quotation marks omitted, alteration accepted).

The seminal Supreme Court case regarding abstract ideas, *Alice Corp. Pty. v. CLS Bank Int'l*, 573 U.S. 208 (2014), outlined the two-step process that courts must

use to assess whether a claimed invention is an unpatentable abstract idea. At *Alice* step one, the Court must determine whether the claims are "directed to" an abstract idea. *Id.* at 217. If they are not, then the inquiry ends, and the court must find that the claims are patent eligible under § 101. If the claims are drawn to an abstract idea, then the court must proceed to *Alice* step two and assess whether the elements of the asserted claim contain an "inventive concept" sufficient to "transform" the abstract idea into a patent-eligible invention. *Id.* at 221. (quoting *Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc.*, 566 U.S. 66, 71 (2012)).

In the absence of clearer guidance from the Supreme Court as to what constitutes an abstract idea, courts may "compare [the] claims at issue to those claims already found to be directed to an abstract idea in previous cases." *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016). This inquiry "must focus on the language of the Asserted Claims themselves . . . considered in light of the specification." *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1292 (Fed. Cir. 2020) (quotation marks and citation omitted). "Subject matter eligibility under § 101 may be determined at the Rule 12(b)(6) stage of a case. Dismissal at this early stage, however, is appropriate only when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law." *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 765 (Fed. Cir. 2019) (quotation marks and citation omitted).

III. ANALYSIS

A. SFI's Motion to Amend the Complaint

SFI seeks to amend the complaint to add claims for willful infringement as to all of the asserted patents. SFI argues that it learned during discovery that Google "met multiple times with SFI's predecessors-in-interest and was on notice of the patented technology at issue in this case." ECF No. 74 at 1. SFI argues that these facts show that "Google has, and continues to, willfully infringe the Asserted Patents." *Id.* at 3.

i. SFI's Allegations of Willful Infringement

The allegations that SFI seeks to add to the complaint are summarized as follows. Beginning in early 2017, Google and Security First Corporation ("SFC")[4] had several meetings and exchanged communications regarding "the possible incorporation of SFC's technology into Google's products and services." ECF No. 75-1 ¶ 45. During those interactions, SFC provided Google with "substantial information" regarding SFC's technology and "informed Google that SFC's technology was patent protected." *Id.* Over two years later, SFC Secured Creditors Trust[5] "made Google aware of SFC's substantial patent portfolio relating to data security technology used

[4] SFC is the "original owner of the Asserted Patents" and "was established in 2002 to develop innovative data security systems." ECF No. 75-1 ¶ 14. "The longtime former chairman of SFC" formed SFI. *Id.* ¶ 17. SFI acquired the asserted patents in 2022. *Id.*

[5] The proposed amended complaint does not explain what relationship SFC Secured Creditors Trust has to SFC and SFI. It appears that SFC Secured Creditors Trust may have been formed, in part, to monetize SFC's patent portfolio after it declared bankruptcy in August 2020. *See* ECF No. 75-1 ¶¶ 55, 59.

by Google." *Id.* At this time, SFC's patent portfolio included the '140 and '854 patents, as well as the published applications that led to the '609 and '116 patents. *Id.*

The proposed amended complaint provides additional details regarding specific interactions between SFC and Google in the 2017–2018 timeframe. ECF No. 75-1 ¶¶ 47–51. For example, it states that on January 30, 2018, individuals from SFC and Google met in California. *Id.* ¶ 49. At that meeting, SFC "presented a slide deck that contained descriptions of how certain of SFC's data security inventions worked, including, among other things, the method that SFC had invented to secure cloud-based data that comprised splitting the data into chunks, encrypting the data with a first encryption key, encrypting the first encryption key with a second encryption key, and storing the first encryption key with the data and the second encryption key in a separate location." *Id.*

According to the proposed amended complaint, "[t]he provisional patent applications for each Asserted Patent were filed in 2004 and 2005, and the non-provision[al] application that led to the '140 patent was publicly available no later than September 3, 2012." ECF No. 75-1 ¶ 52. In addition, the '140 patent issued before the meetings between SFC and Google, and "could have been identified through a simple search on Google's own search engine." *Id.* After several meetings occurred, "Google suddenly went silent." *Id.*

SFC Secured Creditors Trust and Google had several interactions in and around 2021. ECF No. 75-1 ¶¶ 55–59. For example, in February 2021, SFC Secured Creditors Trust emailed Google a presentation "concerning SFC's patent portfolio,

which by that time included the issued '140 and '854 Patents and the published applications that led to the '609 and '116 patents." *Id.* ¶ 55. A revised version of the presentation that was provided later in February "highlighted six patents, including two patents in the same patent family as the '140 and '116 Patents that SFI is asserting in this litigation." *Id.* ¶ 57.

Finally, the proposed amended complaint contends that "at a minimum, Google has had knowledge of the Asserted Patents and Google's infringement of the Asserted Patents since SFI filed its original complaint on March 10, 2023" and "has done nothing to cease its infringement." ECF No. 75-1 ¶ 61.

The proposed amended complaint also alleges other ways that Google knew or should have known of the '140 patent "and other patents and patent applications in the same patent family." ECF No. 75-1 ¶ 53. For example, in 2014, the PTO "rejected a Google patent application" in view of one of SFC's applications, US 2012/0221854. *Id.* The proposed amended complaint states that the '140 patent and '854 application claim priority to the same application and have "materially the same" specifications, including "all quotations from the specification of the '854 Application that the examiner cited in rejecting Google's '196 Application." *Id.*

ii. Merits of SFI's Motion to Amend

Google argues that SFI's motion to amend should be denied because its proposed amendment would be futile.[6] *See* ECF No. 88. To assess futility, courts in the Fourth Circuit apply the Rule 12(b)(6) standard. *Davison*, 912 F.3d at 690. In the

[6] Google does not assert that the amendment would be prejudicial or that SFI's request is being made in bad faith.

wake of *Halo*, the contours of what kind of conduct warrants imposing enhanced damages are somewhat unclear, particularly under the Rule 12(b)(6) standard. *See Sonos, Inc. v. Google LLC*, 591 F. Supp. 3d 638, 643 (N.D. Cal. 2022) ("But what must be *pled* at the outset? No post-*Halo* appellate authority addresses any pleading requirements for enhanced damages, or for that matter, willful infringement.") (emphasis in original). In the absence of definitive guidance from the Federal Circuit, this Court will apply the test articulated in *Dynamic Data Technologies*: "a willful infringement-based claim for enhanced damages survives a motion to dismiss if it alleges facts from which it can be plausibly inferred that the party accused of infringement (1) had knowledge of or was willfully blind to the existence of the asserted patent and (2) had knowledge of or was willfully blind to the fact that the party's alleged conduct constituted, induced, or contributed to infringement of the asserted patent." 2020 WL 4365809, at *5.[7]

a. Pre-Suit Knowledge of the Asserted Patents

As SFI appears to recognize, its proposed amended complaint does not plead any direct evidence that Google was aware of the asserted patents prior to the filing of the original complaint. *See, e.g.*, ECF No. 74 at 10 ("To be sure, the Amended

[7] As the court in *Dynamic Data Technologies* cogently explained, "[b]ecause of the difficulty in articulating precisely the range or type of circumstances that would transform a simple intentional or knowing infringement claim into an enhanced damages claim, the safest course is to allow an enhanced damages claim to proceed beyond the pleadings stage if the operative pleading alleges facts from which it can be plausibly inferred that the party accused of infringement had knowledge of the asserted patent and knowledge that the party's alleged conduct constituted, induced, or contributed to infringement of the asserted patent." 2020 WL 4365809, *5 (quotation marks omitted).

Complaint does not provide *direct* evidence that Google *actually* knew of the specific issuance number of each Asserted Patent.") (emphasis in original). But direct evidence of actual knowledge is not a prerequisite to pleading a willful infringement claim—if that were so, the Supreme Court's "reasonable inference" jurisprudence would have little room to operate. *Iqbal*, 556 U.S. at 678.

Thus, as other courts have recognized, facts sufficient to allow a reasonable inference of knowledge are sufficient to support a pleaded claim for willful infringement. *See, e.g.*, *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1342 (Fed. Cir. 2016) (upholding jury finding that an accused infringer had knowledge of the patents based on "record evidence upon which it could have inferred that [the defendant] had knowledge of the patents at issue"); *Softex LLC v. HP Inc.*, No. 1:22-cv-1311, 2023 WL 2392739, at *2 (W.D. Tex. Mar. 7, 2023) (granting motion to dismiss willful infringement claim because the complaint "fail[ed] to allege any facts to plausibly infer pre-suit knowledge"); *Cirba Inc. v. VMware, Inc.*, No. 1:19-cv-742, 2023 WL 3151852, at *2 (D. Del. Apr. 18, 2023) (granting motion for summary judgment of no willful infringement where there was no evidence "from which a jury could infer *knowledge* of the patent") (emphasis in original); *SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, 396 F. Supp. 3d 323, 334 (S.D.N.Y. 2019) (finding "evidence from which a jury could reasonably infer that [the defendant] had such knowledge").

When the broadly permissive standard for willful infringement post-*Halo* is viewed together with the equally broad and permissive Rule 12(b)(6) standard, the

Court is compelled to find that SFI's motion to amend should be granted. None of the facts pleaded in the proposed amended complaint stands out as particularly strong individually, but when all of the facts are taken together—the number of meetings and communications between SFC (and SFC Secured Creditors Trust); SFC's descriptions of its technology and its repeated statements about its technology being patented; the rejection of a Google patent application over an SFC application with a specification that is "materially the same" as that of the '140 patent, including "all quotations" contained in the examiner's rejection; and the identification of the '140 family of patents by their expiration date and a short description of the subject matter in one of the presentations SFC showed to Google[8]—it is possible to draw the reasonable inference that Google was aware of the '140 patent.[9]

---

[8] The SFC presentation is described in Paragraph 57 of the amended complaint, ECF No. 75-1 ¶ 57, but was not attached to the amended complaint. Instead, Google attached the presentation to its brief in opposition to the motion to amend. ECF No. 91-1. Thus, the Court can only consider the presentation if it finds that it is "integral to the complaint and there is no dispute about the document's authenticity." *Goines v. Valley Cmty. Servs. Bd.*, 822 F.3d 159, 166 (4th Cir. 2016). Because the amended complaint discusses this presentation in detail, and because SFI's claim for willful infringement turns, in part, on the content of the presentation, the Court finds that it is integral to the amended complaint. *See id; see also Defs. of Wildlife v. Boyles*, 608 F. Supp. 3d 336, 344 (D.S.C. 2022) ("A document is integral to a complaint if the claims turn on or are otherwise based on statements contained in the document."). There is no dispute about its authenticity.

[9] On September 20, 2023, SFI filed a notice of supplemental authority which included a series of emails, dated September through October 2017, between SFC and Google. ECF Nos. 100 (notice), 104 (email thread), 105 (email attachment). During the course of those exchanges, SFC sent a list of its patents, including the asserted '140 patent, to Google. ECF No. 105. It is perplexing that SFI did not seek leave to file a second amended complaint in light of this evidence, given that it is stronger evidence of knowledge than anything pleaded in the amended complaint. Because this additional

This evidence places this case in the same ballpark as other cases that have allowed willful infringement claims to proceed. *See, e.g.*, *Kewazinga Corp. v. Microsoft Corp.*, 558 F. Supp. 3d 90, 119 (S.D.N.Y. 2021) (denying summary judgment of no willful infringement because the defendant had knowledge of patents related to the asserted patent and the jury could thus infer knowledge of the asserted patent); *Ocado Innovation, Ltd. v. AutoStore AS*, 561 F. Supp. 3d 36, 57 (D.N.H. 2021) (denying motion to dismiss willful infringement allegations based on, e.g., "the competitive nature" of the industry, the fact that the parties "explored a business relationship" where the plaintiff disclosed technology and patent applications to the defendant, the chronology of the defendant's product development, the defendant's citation of other patents belonging to the plaintiff, and the defendant's patent prosecution activity with respect to other patents belonging to the plaintiff); *SIMO Holdings*, 396 F. Supp. 3d at 334 (denying judgment as a matter of law on a willful infringement claim based on evidence that the defendant was aware of the asserted patent's parent, the application for the asserted patent was pending at the time the defendant was aware of the parent patent, and the defendant's "internal architecture documents" bore "notable similarities" to the asserted patent).

---

evidence is not part of the amended complaint, the Court cannot consider it when assessing whether the proposed amendment would be futile. *U.S. ex rel. Wilson v. Kellogg Brown & Root, Inc.*, 525 F.3d 370, 376 (4th Cir. 2008) (futility assessed under Rule 12(b)(6) standard); *Goldfarb v. Mayor & City Council of Baltimore*, 791 F.3d 500, 508 (4th Cir. 2015) (a court's review of a complaint under Rule 12(b)(6) is ordinarily limited to the facts in the complaint); *Cano v. DPNY, Inc.*, 287 F.R.D. 251, 257 (S.D.N.Y. 2012) (refusing to consider evidence submitted in opposition to motion to amend complaint because "futility is generally adjudicated without resort to any outside evidence.") (quotation marks omitted, alteration accepted).

SFI has not pleaded sufficient facts to support a reasonable inference that Google was aware of the other asserted patents. The '854 and '609 patents were not identified by family expiration date in the SFC presentation, nor were they related to the SFC application cited in the prosecution of Google's application.[10] Indeed, none of the nonprovisional applications for the other asserted patents had even been filed at the time of the rejection. Given that the inference established with respect to the '140 patent already hangs by the barest thread, the lack of these pieces of evidence for the '854, '609, and '116 patents renders any inference of knowledge unreasonable.

Google cites cases where courts have, in other contexts, rejected the kinds of evidence of knowledge contained in the proposed amended complaint.[11] However, as the Court explained above, it is the *combination* of evidence in this case that allows the inference of knowledge to be reasonable. These cases are also distinguishable.

---

[10] Because the '140 and '116 patents share a specification, one could argue that this evidence should apply to the '116 patent as well. But because the nonprovisional application for the '116 patent had not even been filed at the time of the PTO's rejection of Google's application, such a finding would be a bridge too far. ECF No. 75-1 ¶ 52 (noting that "provisional patent application for each Asserted Patent were filed in 2004 and 2005"); '116 patent (noting that application was filed on May 11, 2018).

[11] *See, e.g.*, *State Indus., Inc. v. A.O. Smith Corp.*, 751 F.2d 1226, 1236 (Fed. Cir. 1985); *Biedermann Techs. GmbH & Co. KG v. K2M, Inc.*, 528 F. Supp. 3d 407, 426 (E.D. Va. 2021); *Virginia Innovation Scis., Inc. v. Samsung Elecs. Co.*, 983 F. Supp. 2d 700, 710 (E.D. Va. 2013); *Software Rsch., Inc. v. Dynatrace LLC*, 316 F. Supp. 3d 1112, 1133 (N.D. Cal. 2018); *Dental Monitoring SAS v. Align Tech., Inc.*, No. 3:22-cv-7335, 2023 WL 4297570, at *6 (N.D. Cal. June 30, 2023); *Kirsch Rsch. & Dev., LLC v. Tarco Specialty Prod., Inc.*, No. 6:20-cv-00318, 2021 WL 4555802, at *2 (W.D. Tex. Oct. 4, 2021); *NetFuel, Inc. v. Cisco Sys. Inc.*, No. 5:18-cv-02352, 2018 WL 4510737, at *2 (N.D. Cal. Sept. 18, 2018); *Vasudevan Software, Inc. v. TIBCO Software Inc.*, No. 3:11-cv-6638, 2012 WL 1831543, at *3 (N.D. Cal. May 18, 2012).

For example, *Dental Monitoring*, *Biedermann*, *State Industries*, *Kirsch Research*, and *Virginia Innovation* are distinguishable because those cases lack some of the additional pleaded evidence here, including the rejection of one of the patentee's own patents over a related application and the identification of a family of asserted patents by their expiration date. *Biedermann* and *State Industries* were also decided against different evidentiary standards: summary judgment and an appeal from a final judgment on the merits, respectively.

In *NetFuel*, the court's decision was based in part on the fact that, at the time of the interactions between the patentee and accused infringer, the patent had not yet issued, and the available application was provisional, meaning it did not contain claims. Similarly, in *Vasudevan Software*, the asserted patent had not yet issued at the time of the relevant interactions. But here, the '140 patent had issued by the time of SFC's interactions with Google.

Software Research is also distinguishable because two of the notice letters considered by that court "were sent nearly a decade ago to other companies [i.e., not the defendant]," and the letters were sent before the asserted patent existed. *Software Research*, 316 F. Supp. 3d at 1133. Here, the interactions described in the proposed amended complaint involved Google, not "other companies," and those interactions occurred entirely after the '140 patent was issued in May 2016.

Accordingly, SFI has pleaded facts sufficient to allow the plausible inference that Google was aware of the '140 patent prior to the filing of this suit, but was not aware of the other asserted patents.

b. Pre-Suit Knowledge of Infringement

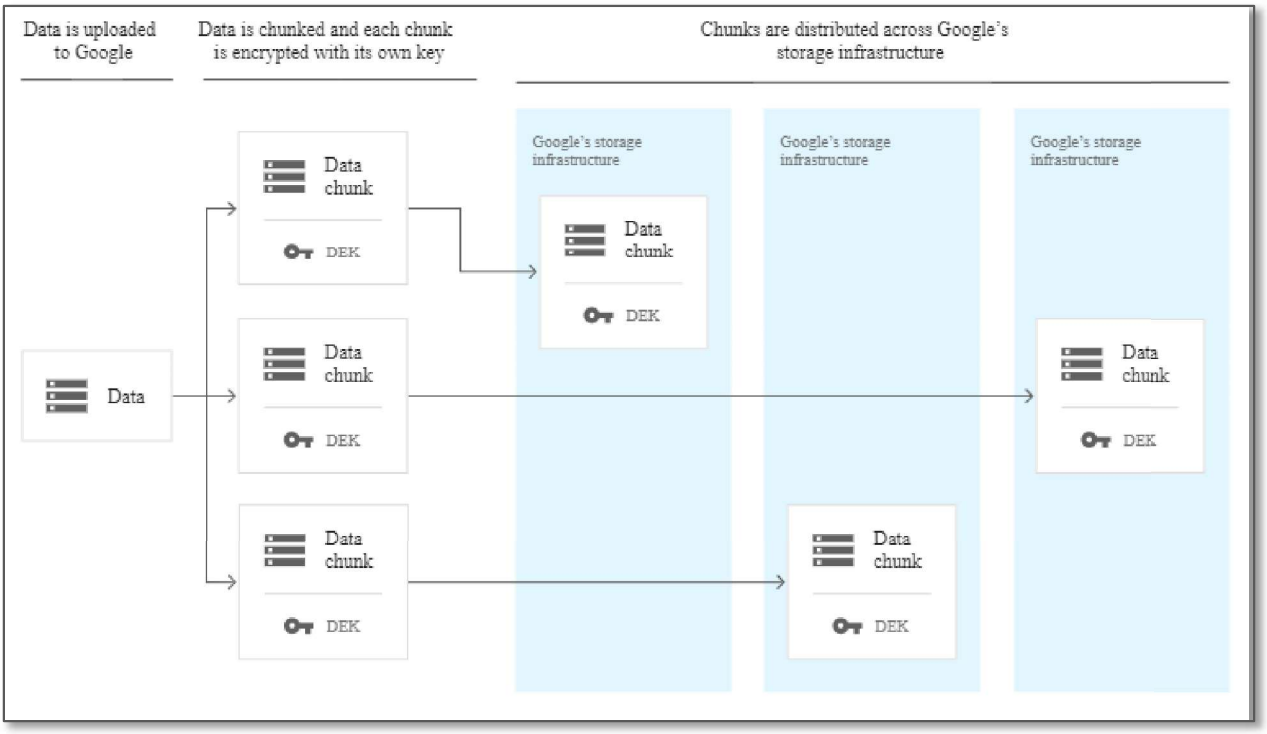
SFI must also plead that Google "had knowledge of or was willfully blind to the fact that [its] alleged conduct constituted, induced, or contributed to infringement of the asserted patent." *See, e.g.*, *Dynamic Data Techs.*, 2020 WL 4365809, at *5. SFI argues that the facts pleaded in the complaint "give rise to a plausible *inference* that Google actually knew of . . . Google's probable infringement," pointing to, *inter alia*, the interactions between SFC and Google, "the content and detail of the technical information disclosed by SFC to Google," and the "substantial similarity" between the technology SFC disclosed and Google's encryption technology. ECF No. 74 at 10–11 (emphasis in original).

According to the proposed amended complaint, SFC's discussions with Google included a recitation of the basic steps claimed in the asserted patents:

> On or about January 30, 2018, Messrs. Mumaugh and Viehweg met with Mr. Bhan at Google's offices in Sunnyvale, California. During that meeting, Messrs. Mumaugh and Viehweg presented a slide deck that contained descriptions of how certain of SFC's data security inventions worked, including, among other things, the method that SFC had invented to secure cloud-based data that comprised splitting the data into chunks, encrypting the data with a first encryption key, encrypting the first encryption key with a second encryption key, and storing the first encryption key with the data and the second encryption key in a separate location. In short, a data security method that was substantially similar to Google's Encryption At-Rest technology.

ECF No. 75-1 ¶ 49. The proposed amended complaint's description of Google's Encryption At-Rest technology is largely consistent with SFC's description of its technology. For example, the proposed amended complaint describes Google's

encryption process using the following diagram, which shows that Google's process breaks data into chunks, encrypts the chunks with their "own" keys, and then stores the chunks with the keys on various storage devices:



ECF No. 75-1 at 14. It also explains that the individual encryption keys employed by Google are further encrypted with an additional "key encryption key." *Id.* ¶ 41. These steps are consistent with the basic steps claimed by the asserted patents and described by SFC in its January 2018 meeting with Google.[12]

[12] Claim 1 of the '140 patent differs from the other asserted patents because it includes limitations relating to a "virtual disk." *See* '140 patent, claim 1. The proposed amended complaint's description of the pre-suit interactions between SFC and Google does not indicate whether these limitations were part of SFC's description of its patented technology. Nonetheless, because the pleaded facts support an inference of knowledge of or willful blindness to the '140 patent, the facts also support an inference of knowledge of or willful blindness to what that patent claims. And the proposed amended complaint's infringement allegations with respect to the "virtual

Based on the facial similarity between the proposed amended complaint's characterization of Google's technology and the asserted patented technology (as discussed above), the Court finds that one may plausibly infer that Google had "knowledge of or was willfully blind to the fact that [their] alleged conduct constituted, induced, or contributed to infringement of the asserted patent." *Dynamic Data*, 2020 WL 4365809, at *5.

c. Post-Suit Willful Infringement

SFI also alleges that "Google's infringement of the Asserted Patents has been willful since the service of the original complaint on March 10, 2023." ECF No. 74 at 16; ECF No. 75-1 ¶ 61. Whether a complaint can supply the necessary knowledge to support a claim of willful infringement is a question that has divided district courts. *Compare, e.g.*, *ZapFraud, Inc. v. Barracuda Networks, Inc.*, 528 F. Supp. 3d 247, 248 (D. Del. 2021) (holding that a complaint cannot serve as notice for willful infringement and collecting cases) *and Rembrandt Social Media, LP v. Facebook, Inc.*, 950 F. Supp. 2d 876 (E.D. Va. 2013) (same) *with BillJCo, LLC v. Cisco Sys., Inc.*, No. 2:21-cv-00181, 2021 WL 6618529, at *8 (E.D. Tex. Nov. 30, 2021) (holding that a complaint can serve as notice for willful infringement).

In *Rembrandt*, the Honorable T. S. Ellis III held that service of a complaint does not provide notice adequate to support a claim of willful infringement.

---

disk" element cite evidence from 2018 and 2020, which is fairly contemporaneous with SFC's discussions with Google. ECF No. 75-1 ¶¶ 154–55. Therefore, the facts alleged in the amended complaint support a plausible inference that Google knew of or was willfully blind to its infringement of each limitation of claim 1 of the '140 patent before the commencement of this suit.

Rembrandt, 950 F. Supp. 2d at 884. Judge Ellis explained that "[t]o conclude otherwise would lead to the anomalous result that every lawsuit alleging infringement could include a willful infringement claim based on simply the filing or the serving of a complaint."[13] *Id.* In *ZapFraud,* the court held the same, reasoning that "[t]he purpose of a complaint is to obtain relief from an existing claim and not to create a claim." *ZapFraud*, 528 F. Supp. 3d at 250 (quoting *Helios Streaming, LLC v. Vudu, Inc.*, No. 1:19-cv-1792, 2020 WL 3167641, at *2 n.1 (D. Del. June 15, 2020)). The court explained further:

> ZapFraud has identified, and I know of, no area of tort law other than patent infringement where courts have allowed a plaintiff to prove an element of a legal claim with evidence that the plaintiff filed the claim. The limited authority vested in our courts by the Constitution and the limited resources made available to our courts by Congress counsel against encouraging plaintiffs to create claims by filing claims. It seems to me neither wise nor consistent with principles of judicial economy to allow court dockets to serve as notice boards for future legal claims for indirect infringement and enhanced damages.

Id. In *Callwave Commc'ns LLC v. AT & T Mobility LLC*, No. 1:12-cv-1701, 2014 WL 5363741 (D. Del. Jan. 28, 2014), the court reasoned that not allowing "allegations of willfulness based solely on conduct post-dating the filing of the original complaint" would encourage parties to provide pre-suit notice of infringement allegations, which brings "a benefit to society if the matter is resolved without a suit." *Id.* at *1.

---

[13] The court's decision on this issue in *Rembrandt* rested in part on the Federal Circuit's holding in *In re Seagate Tech., LLC,* 497 F.3d 1360 (Fed. Cir. 2007), which was subsequently vacated by the Supreme Court in *Halo*. *Rembrandt*, 950 F. Supp. 2d at 883–84. To be clear, the Court's reliance on *Rembrandt* is limited solely to the reasoning quoted above, which remains applicable and persuasive after *Halo*.

The Court finds the reasoning of the courts in *Rembrandt, ZapFraud,* and *Callwave* persuasive and, consistent with those cases, holds that a complaint cannot provide the notice necessary to establish knowledge for willful infringement purposes.

SFI argues that the Court need not resolve "the metaphysical question of whether a patent owner can allege willful infringement in an original complaint based on the filing of that same original complaint" because, here, the allegation of willful infringement is being made in an *amended* complaint. ECF No. 93 at 15. SFI's argument emphasizes form at the expense of substance. The question before the Court is still whether a complaint—operative at the time it is filed and served—can supply the necessary knowledge for a willful infringement allegation. Consistent with the Court's discussion above, the answer is still no, even when a plaintiff has filed an amended complaint. *See Callwave*, 2014 WL 5363741, at *1 (noting that the plaintiff alleged willfulness based on service of "an earlier version of the suit . . . before the present amended complaint was filed" and holding that such notice is insufficient for willful infringement). Permitting plaintiffs to assert post-suit willful infringement in amended complaints but *not* in original complaints would incentivize plaintiffs to file amended complaints, which would unduly burden litigants and the courts.[14]

[14] Conversely, this holding does not incentivize post-complaint infringement or leave patentees without a remedy for such infringement—patentees can seek damages for "past and future infringement through the life of the patent," *Summit 6, LLC v. Samsung Elecs. Co.*, 802 F.3d 1283, 1301 (Fed. Cir. 2015), and the court may award supplemental damages for infringement "not covered by [a] jury verdict," *ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, No. 2:10-cv-248, 2011 WL 4899922, at *4 (E.D. Va. Oct. 14, 2011), *aff'd*, 694 F.3d 1312 (Fed. Cir. 2012).

d. Egregious Behavior

The parties dispute whether SFI was required to plead facts indicating that Google engaged in "egregious" conduct[15] that would warrant an award of enhanced damages. ECF No. 88 at 22–24; ECF No. 93 at 14. This question, too, has divided district courts. *See, e.g.*, *Valinge Innovation AB v. Halstead New England Corp.*, No. CV 1:16-cv-1082, 2018 WL 2411218, at *6 (D. Del. May 29, 2018) (holding that egregious conduct is not an element of a willful infringement claim); *Finjan, Inc. v. Cisco Sys. Inc.*, No. 5:17-cv-72, 2017 WL 2462423, at *5 (N.D. Cal. June 7, 2017) (dismissing allegation of willful infringement because the complaint failed to plead egregious conduct).

The Federal Circuit's post-*Halo* jurisprudence suggests that a plaintiff is not required to plead such egregious conduct in the complaint. For example, in *Eko Brands, LLC v. Adrian Rivera Maynez Enterprises, Inc.*, 946 F.3d 1367 (Fed. Cir. 2020), the court explained that "[u]nder *Halo*, the concept of 'willfulness' requires a jury to find no more than deliberate or intentional infringement." *Id.* at 1378 (quoting *Halo*, 579 U.S. at 94). The court then explained that "[t]he question of enhanced damages is addressed by the court once an affirmative finding of willfulness has been made." *Id.* The court concluded that "whether an accused patent infringer's conduct was 'egregious behavior' or 'worthy of punishment' are therefore not appropriate for jury consideration." *Id.*

[15] Throughout this Memorandum Opinion and Order, the Court uses "egregious conduct" as a shorthand to refer to the factual circumstances that "transform[] simple knowledge into such egregious behavior" and warrant imposing enhanced damages. *Halo*, 579 U.S. 93, 111 (Breyer, J., dissenting).

Eko Brands demonstrates that the willfulness inquiry is separate from the egregious conduct inquiry, which supports the proposition that a finding of egregious conduct is not needed to find willfulness. This is further supported by the court's discussion in *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 14 F.4th 1323 (Fed. Cir. 2021), where the Court clarified that *Halo*'s reference to "wanton, malicious, and bad-faith" conduct refers to "'conduct warranting enhanced damages,' not conduct warranting a finding of willfulness." *Id.* at 1330 (quoting *Halo*, 579 U.S. at 103–04). The court then proceeded to analyze willful infringement separately from enhanced damages. *Id.* at 1330–31. The court also clarified that "willfulness is a component of enhancement," and a finding of willfulness does not necessarily warrant enhanced damages. *Id.*

More recently, in *Ironburg Inventions Ltd. v. Valve Corp.*, 64 F.4th 1274 (Fed. Cir. 2023), the Federal Circuit considered whether the district court erred when it denied the defendant's motion for judgment as a matter of law of no willful infringement because the district court had already decided "it was not going to exercise its discretion to enhance infringement damages." *Id.* at 1295. The Federal Circuit concluded that this was error, noting that "[w]illfulness and enhancement are separate issues . . . and a finding of willful infringement may have collateral consequences even for a party not ordered to pay enhanced damages, such as reputational injuries and possible nondischargeability of debts in bankruptcy." *Id.* (citations omitted).

Eko Brands, SRI International, and *Ironburg Inventions* show that willful infringement and egregious conduct are distinct but parallel inquiries that must both

be answered in the affirmative to award enhanced damages. Put another way, a plaintiff may show that a defendant willfully infringed their patent without showing that the defendant acted egregiously in a way that warrants imposing enhanced damages; in such a case, the plaintiff has still succeeded on their willful infringement claim. *See, e.g.*, *Ironburg Inventions*, 64 F.4th at 1295.

Consistent with the decisions of other district courts that have addressed this question, the Court finds that egregious conduct is not an element of a claim for willful infringement that needs to be pleaded in the complaint.[16] *See, e.g.*, *Fate Therapeutics, Inc. v. Shoreline Biosciences, Inc.*, No. 22-cv-00676, 2023 WL 2756494,

[16] Google cites *Bushnell Hawthorne, LLC v. Cisco Sys., Inc.*, No. 1:18-cv-760, 2019 WL 8107921 (E.D. Va. Feb. 26, 2019), for the proposition that a complaint must plead that an alleged infringer's conduct was egregious. ECF No. 88 at 16. In that case, the court explained that "to state a plausible claim of willful infringement, the complaint must also allege facts to demonstrate the defendant's behavior was egregious under the circumstances, such as facts showing that defendant was subjectively aware of the risk that its conduct constituted infringement." *Bushnell*, 2019 WL 8107921, at *1. To this Court—which has the benefit of the Federal Circuit's more recent decisions in *Eko Brands*, *SRI International*, and *Ironburg Inventions*—it appears that the court in *Bushnell* lumped together the knowledge of infringement prong of the willfulness inquiry and the egregious conduct inquiry. But, as that court explained, an accused infringer's "egregious" behavior can include "subjective[] aware[ness] of the risk that its conduct constituted infringement," which is similar to the knowledge of infringement inquiry undertaken by the Court here. *Id.* In this way, this Court's conclusion is largely consistent with *Bushnell*, insofar as the *Bushnell* court did not necessarily require the plaintiff to plead anything more than the defendant's knowledge of the asserted patent(s) and knowledge of its infringement. This Court agrees with the *Bushnell* court that a claim for enhanced damages proceeding on a willful infringement theory needs to show some kind of knowledge of or willful blindness to infringement on the part of the accused infringer. Where this Court and the *Bushnell* court disagree is whether the facts that "transform[] simple knowledge into such egregious behavior [that warrants enhanced damages]" must be pleaded in the complaint. *Halo*, 579 U.S. at 111 (Breyer, J., concurring). In this Court's view, the Federal Circuit's recent decisions have established that those facts may be shown later.

at *10 (S.D. Cal. Mar. 30, 2023); *Therabody, Inc. v. Tzumi Elecs. LLC*, No. 21-cv-7803, 2022 WL 17826642, at *5 (S.D.N.Y. Dec. 19, 2022); *Sonos*, 591 F. Supp. 3d at 644; *Align Tech., Inc. v. 3Shape A/S*, 339 F. Supp. 3d 435, 448 (D. Del. 2018); *Dresser, LLC v. VRG Controls, LLC*, No. 18-cv-1957, 2018 WL 10426611, at *4 (N.D. Ill. Nov. 28, 2018); *Valinge Innovation*, 2018 WL 2411218, at *6.

* * *

Accordingly, SFI's motion to amend is granted. SFI's willful infringement claim as to the '140 patent may proceed, but its willful infringement claims as to the remaining asserted patents may not.

B. Google's Motion to Dismiss

Google argues that "the Asserted Claims are directed to ineligible subject matter" under § 101 because, at *Alice* step one, the patents are "directed to the abstract idea of parsing and encrypting stored data" and "disclose no *specifics* for how to implement the otherwise functional steps of the claims" and, at *Alice* step two, "they merely recite abstract, routine, conventional activities done with generic computer hardware and software." ECF No. 38 at 8 (emphasis in original).

Because the Federal Circuit has indicated that district courts may "compare [the] claims at issue to those claims already found to be directed to an abstract idea in previous cases," *Enfish*, 822 F.3d at 1335, the Court will first provide an overview of several relevant Federal Circuit cases. Then, the Court will compare the claimed inventions in those cases to the invention claimed by the asserted patents here to determine whether the asserted claims are directed to an abstract idea.

i. Alice *and the Federal Circuit's Application of the* Alice *Two-Step Framework*

a. Cases where the asserted claims were found to be directed to ineligible subject matter under § 101

In *Alice* itself, the patents related to "a computerized scheme for mitigating 'settlement risk'—i.e., the risk that only one party to an agreed-upon financial exchange will satisfy its obligation." *Alice*, 573 U.S. at 213. The Court summarized the claims as: "(1) the foregoing method for exchanging obligations (the method claims), (2) a computer system configured to carry out the method for exchanging obligations (the system claims), and (3) a computer-readable medium containing program code for performing the method of exchanging obligations (the media claims)." *Id.* at 214.

At step one, the Court found the asserted claims were directed to an abstract idea. The Court found that the claims were "drawn to the concept of intermediated settlement," which "is a fundamental economic practice long prevalent in our system of commerce." *Alice*, 573 U.S. at 219 (quotation marks omitted). At step two, the Court found that "the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." *Id.* at 223. The Court found that each step of the function the computer performed was a "purely conventional" step "previously known to the industry."[17] *Id.* at 225 (quotation marks omitted, alteration accepted).

[17] The Court's analysis at *Alice* step two echoes the concept of patent novelty. Courts have attempted to explain the difference between the "inventive feature" inquiry under § 101 and the novelty inquiry under §§ 102 and 103. *See, e.g.*, *Cogent Med., Inc.*

In *Ericsson Inc. v. TCL Commc'n Tech. Holdings Ltd.*, 955 F.3d 1317 (Fed. Cir. 2020), the patent before the Federal Circuit described "a system and method for controlling access to a platform for a mobile terminal for a wireless telecommunications system." *Id.* at 1325 (quotation marks omitted). At *Alice* step one, the court found that "[a]lthough written in technical jargon, a close analysis of the claims reveals that they require nothing more than" the "abstract idea" of "controlling access to, or limiting permission to, resources." *Ericsson*, 955 F.3d at 1326. The court reasoned that "[c]ontrolling access to resources is exactly the sort of process that can be performed in the human mind, or by a human using a pen and paper, which we have repeatedly found unpatentable." *Id.* (quotation marks omitted).

At *Alice* step two, the patentee argued that the "layered architecture" feature of the invention constituted an inventive concept. *Ericsson*, 955 F.3d at 1328 (quotation marks omitted). The court rejected that argument, noting that "this allegedly novel aspect of the invention is wholly missing from" the asserted claims, and that "[n]either claim recites any particular architecture at all—much less the specific three-layered architecture advocated by Ericsson." *Id.*

In *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342 (Fed. Cir. 2021), the patents before the Federal Circuit were "unrelated" but all dealt with "similar

---

v. Elsevier Inc., 70 F. Supp. 3d 1058, 1065 n.3 (N.D. Cal. 2014). Ultimately, while there may be some conceptual overlap, they are treated differently as a matter of doctrine, and a finding in one area does not impact the other. *See, e.g.*, *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1151 (Fed. Cir. 2016) ("[A] claim for a *new* abstract idea is still an abstract idea. The search for a § 101 inventive concept is thus distinct from demonstrating § 102 novelty.") (emphasis in original).

technology—securing electronic payment transactions." *Id.* at 1345. The '539 patent contemplated the creation of a "Universal Secure Registry" ("USR") that takes the place of "multiple conventional forms of identification." *Id.* at 1348 (quotation marks omitted). In one embodiment of the invention, the invention facilitates "purchasing goods or services without revealing personal financial information to a merchant." *Id.* To do so, the patent described a process by which verification codes were passed between the user, merchant, and USR system. *Id.*

At *Alice* step 1, the court found that the asserted claims were directed to an abstract idea. The Court found that "the claims simply recite conventional actions in a generic way (e.g., receiving a transaction request, verifying the identity of a customer and merchant, allowing a transaction) and do not purport to improve any underlying technology." *Universal Secure Registry*, 10 F.4th at 1349 (quotation marks omitted).

At *Alice* step two, the patentee argued that the "claim's recitation of (1) time-varying codes and (2) sending data to a third-party as opposed to the merchant each rise to the level of an inventive concept." *Universal Secure Registry*, 10 F.4th at 1350. The court rejected both arguments, noting that "the patent itself acknowledges that the claimed step of generating time-varying codes for authentication of a user is conventional and long-standing," and that the Supreme Court in *Alice* had held that "the use of a third-party intermediary in a financial transaction" is an abstract idea. *Id.*

b. Cases where the asserted claims were found to be directed to eligible subject matter under § 101

In *Enfish*, the patents before the Federal Circuit were "directed to an innovative logical model for a computer database" which is a "model of data for a computer database explaining how the various elements of information are related to one another." *Enfish*, 822 F.3d at 1330. The claimed logical model "include[d] all data entities in a single table, with column definitions provided by rows in that same table," which was contrary to conventional logical models at the time that stored each kind of data in a separate table. *Id.*

At *Alice* step one, the Court found that the claims were not directed to an abstract idea. "Rather, they are directed to a specific improvement to the way computers operate, embodied in the self-referential table." *Enfish*, 822 F.3d at 1336. The court rejected the district court's characterization of the claimed invention, which it said was "storing, organizing, and retrieving memory in a logical table" and "the concept of organizing information using tabular formats." *Id.* at 1337 (quotation marks omitted). The court noted that "describing the claims at such a high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule." *Id.* The court reasoned that "the claims are not simply directed to *any* form of storing tabular data, but instead are specifically directed to a *self-referential* table for a computer database." *Id.* (emphasis in original). The court also concluded that the patents' specification disclosed several advantages of the claimed invention over the prior art. *Id.* The court declined to proceed to *Alice* step two.

In *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253 (Fed. Cir. 2017), the patent before the Federal Circuit explained that conventional computer systems used a three-tiered system of memory: low-speed memory for large amounts of data (e.g., a hard drive); medium-speed memory as the main memory (e.g., RAM); and high-speed memory that serves as processor cache memory. *Id.* The patent described various problems with the state of the art: cache memory was the fastest but was not always large enough to store all of the data needed by the processor; transferring data between the types of memory caused delays; and memory systems had to be designed for a particular processor. *Id.* The patent claimed an improved "memory system with programmable operational characteristics that can be tailored for use with multiple different processors." *Id.* at 1255.

The district court found the patents ineligible under *Alice*, concluding that "the claims were directed to the abstract idea of categorical data storage, which humans have practiced for many years." *Id.* (quotation marks omitted). At step two, the district court found no inventive concept because the claimed computer elements "were generic and conventional." *Id.*

At *Alice* step one, the Federal Circuit found that the claims were not directed to an abstract idea. The court concluded that "[n]one of the claims recite all types and all forms of categorical data storage." *Visual Memory*, 867 F.3d at 1259. The court also looked to the specification, which "explains that multiple benefits flow from the . . . improved memory system." *Id.* The court found that "the claims here are directed

to a technological improvement: an enhanced computer memory system." *Id.* The court declined to proceed to *Alice* step two.

In *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018), one of the patents before the court dealt with "a system and method for providing computer security by attaching a security profile to a downloadable." *Id.* at 1302. According to the court, "Claim 1 of the . . . patent scans a downloadable and attaches the virus scan results to the downloadable file in the form of a newly generated file." *Id.* at 1304.

At *Alice* step one, the court found that the claims were not directed to an abstract idea. The court found that "the method of claim 1 employs a new kind of file that enables a computer security system to do things it could not do before." *Id.* at 1305. Thus, the court found that "[t]he asserted claims are [] directed to a non-abstract improvement in computer functionality, rather than the abstract idea of computer security writ large." *Id.* The court declined to proceed to *Alice* step two.

In *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343 (Fed. Cir. 2018), the patent before the Federal Circuit described an improved method for identifying and restricting an unauthorized software program's operation. The method used "a modifiable part of the BIOS memory" to store the information used "to determine whether the program is licensed to run on that computer." *Id.* at 1345. This method "improves computer security" because "successfully hacking BIOS memory . . . is much harder than hacking" conventional computer memory. *Id.* The district court applied *Alice* and granted the defendant's motion to dismiss. *Id.* at 1346.

At *Alice* step one, the court determined that the claims were not directed to an abstract idea. The court found that "[i]mproving security—here, against a computer's unauthorized use of a program—can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem." *Ancora*, 908 F.3d at 1348. The court reasoned that the patent "specifically identifies how that functionality improvement is effectuated in an assertedly unexpected way" and "addresses a technological problem with computers." *Id.* at 1349. The court declined to proceed to *Alice* step two.

In *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278 (Fed. Cir. 2020), the patents before the Federal Circuit claimed "particular systems and methods for multi-level security of various kinds of files being transmitted in a data network." *Id.* at 1282. The patents claimed a method "in which a digital object . . . is assigned a level of security that corresponds to a certain combination of access controls and encryption," and the encrypted object is then "embedded or nested within a container object, which, if itself encrypted and access controlled, provides a second layer of security." *Id.* (quotation marks omitted). The district court below denied the defendant's motion for summary judgment on § 101 ineligibility. *Id.* at 1292.

At *Alice* step one, the Court found that the claims were not directed to an abstract idea but were instead "directed to improving a basic function of a computer data-distribution network, namely, network security." *Id.* at 1296. The court also observed that "[t]he patent makes clear that the focus of the claimed advance is on improving such a data network for broadcasting a file to a large audience, with the

improvement assertedly being an efficient way for the sender to permit different parts of the audience to see different parts of the file." *Id.* The court declined to proceed to *Alice* step two.

ii. Comparing the Asserted Claims to Claims Previously Analyzed by Other Courts

a. Alice *Step One*

At *Alice* step one, the Court must determine "whether the claims at issue are directed to" an abstract idea. *Alice*, 573 U.S. at 217. To determine what the asserted claims are "directed to," the Court asks "what the patent[s] assert[] to be the focus of the claimed advance over the prior art," focusing on "the language of the Asserted Claims themselves . . . considered in light of the specification." *TecSec*, 978 F.3d at 1292 (quotation marks and citation omitted).

Google argues that "the Asserted Claims are directed to the abstract idea of parsing and encrypting stored data." ECF No. 38 at 15. In support, Google asserts that the claim language "is recited in highly generic terms." *Id.* Google analogizes the elements of claim 1 of the '609 patent to storing documents in file cabinets:

1. A method for securing data, the method comprising: executing code by a processor to perform:	
receiving a first key from a storage system;	Obtaining a key for a manager's safe that contains the keys to the office file cabinets
generating a plurality of data chunks based on a data set, wherein each data chunk of the plurality of data chunks comprises less than an entirety of data of the data set, and wherein the data set can be reconstructed using at least a	Dividing a document into sets of pages to be stored in different file cabinets within the office, where the document can be reconstructed using pages from at least a minimum number of file cabinets

minimum number of the plurality of chunks;	
encrypting each respective data chunk of the plurality of data chunks with a respective second key, wherein each of the respective second keys are distinct from each other;	Locking each set of pages into a different file cabinet, each of which has its own key
performing a cryptographic operation based on the first key to further secure the plurality of data chunks; and	Locking the file cabinet keys in the manager's safe using the safe key
storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one storage device.	Posting a note on one or more of the office file cabinets indicating that the key to that file cabinet is in the manager's safe, or that the manager has the key

ECF No. 38 at 21–22. Thus, according to Google, "the recited functions of [the] '609 patent claim 1 could be performed manually by humans." *Id*; *see also Ericsson*, 955 F.3d at 1357 ("Controlling access to resources is exactly the sort of process that can be performed in the human mind, or by a human using a pen and paper, which we have repeatedly found unpatentable.") (quotation marks omitted).

Google's own tortured analogy demonstrates why this case is unlike *Ericsson*. In *Ericsson*, the Federal Circuit held that a patent was directed to "[c]ontrolling access to resources," which was "exactly the sort of process that can be performed in the human mind, or by a human using a pen and paper" and which "long predate[d]" the patent and was "pervasive in human activity." *Ericsson*, 955 F.3d at 1327 (quotation marks omitted).

The sequence of events that Google describes in its analogy is far from "pervasive in human activity"—it is not reasonable or practical to divide documents

into "chunks" of pages, lock those "chunks" in separate places with separate keys, lock those keys away with a separate key, and then "[p]ost[] a note . . . indicating that the key to that file cabinet is in the manager's safe, or that the manager has the key." ECF No. 38 at 21–22. Virtually any computer-based process could be characterized in such a convoluted way. In *TecSec,* for example, the Federal Circuit found the asserted claim was not directed to an abstract idea. *TecSec*, 978 F.3d at 1294–95. But one can easily imagine adapting Google's file cabinet analogy to the claim in *TecSec*:

1. A method for providing multi-level multimedia security in a data network, comprising the steps of:	
A) accessing an object-oriented key manager;	Speaking to the office manager, who manages the keys to the filing cabinets in the office[18]
B) selecting an object to encrypt;	Selecting a document to store in a filing cabinet
C) selecting a label for the object;	Naming the document
D) selecting an encryption algorithm;	Selecting a filing cabinet
E) encrypting the object according to the encryption algorithm;	Locking the document in the filing cabinet
F) labelling the encrypted object;	Naming the file cabinet
G) reading the object label;	Reading the name of the document
H) determining access authorization based on the object label; and	Determining whether employees may access the document based on the name of the document
I) decrypting the object if access authorization is granted.	Unlocking the filing cabinet if the employee may access the document

[18] *See TecSec, Inc. v. Adobe Sys. Inc.*, 658 F. App'x 570, 580 (Fed. Cir. 2016) (construing "Object-oriented Key Manager" to mean "a software component that manages the encryption of an object by performing one or more of the functions of generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys."). All of these are functions that could be performed by a person with physical keys.

TecSec, 978 F.3d at 1282. Indeed, Google's analogy fits the claim at issue in *TecSec* better than the asserted claims here, and the Federal Circuit still found that the claim was non-abstract.

A method claim is not abstract just because it can be analogized to something that can be done in the physical world—after all, real-world methods and processes can be patentable. Instead, to be found ineligible, a method claim must, for example, encompass a process that "long predates the [asserted patent] and is pervasive in human activity," *Ericsson*, 955 F.3d at 1327, or it must claim "some business practice known from the pre-Internet world," *DDR Holdings*, 773 F.3d at 1257. Here, the steps embodied in the asserted claims are virtually nonsensical—or, at the very least, entirely impractical—*except* in the context of computers, which supports the proposition that the claims are directed to an improvement in computer functionality.

The Federal Circuit's decisions in *Ancora* and *Finjan* also support this proposition. The claims in *Ancora* were directed to a method for storing information in the BIOS memory of a computer to "improve[] computer security." *Ancora*, 908 F.3d at 1345. The court explained, at *Alice* step one, that "[i]mproving security . . . can be a non-abstract improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem" and the patent "specifically identifies how that functionality improvement is effectuated in an assertedly unexpected way." *Id.* at 1348–49. In *Finjan*, the court held that the claims were "directed to a non-abstract improvement in computer functionality, rather than the abstract idea of computer security writ large." *Finjan*, 879 F.3d at 1305.

TecSec, Ancora, and *Finjan* show that specific methods for improving computer security can be non-abstract. In the instant case, the claims are directed to an improved method for securely storing data, and the claims themselves explain "how that functionality improvement is effectuated" with specific parsing, encryption, and storage steps. *Ancora*, 773 F.3d at 1348–49.

This conclusion is further bolstered by *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014), where the Federal Circuit found:

> The claims here are similar to the claims in the cases [where the claims were found ineligible as abstract ideas] in the sense that the claims involve both a computer and the Internet. But these claims stand apart because they do not merely recite the performance of *some business practice known from the pre-Internet world* along with the requirement to perform it on the Internet. Instead, the claimed solution is *necessarily rooted in computer technology* in order to overcome a problem specifically arising in the realm of computer networks.

Id. at 1257 (emphasis added). Here, too, the claimed invention is "necessarily rooted in computer technology" because it solves a problem that arises in the context of computers and computer networks. In other words, the patents claim "a technological improvement to computer functionality itself." *Universal Secure Registry*, 10 F.4th at 1350.

In several cases, when considering whether the claims at issue were directed to an abstract idea, the Federal Circuit has analyzed whether the claims purport to cover the whole idea to which they are directed. If they do, they are more likely to be abstract. For example, in *Visual Memory*, the district court found the asserted claims ineligible at *Alice* step one because "the claims were directed to the abstract idea of

categorical data storage, which humans have practiced for many years." *Visual Memory*, 867 F.3d at 1257. But the Federal Circuit reversed, finding that "[n]one of the claims recite all types and all forms of categorical storage." *Id.* at 1259. Similarly, in *Enfish*, the district court found the claims abstract because they were directed to "the concept of organizing information using tabular formats," but the Federal Circuit disagreed, finding that "the claims are not simply directed to *any* form of storing tabular data, but instead are *specifically* directed to a self-referential table for a computer database." *Enfish*, 822 F.3d at 1337 (emphasis added).

Even if you accept Google's characterization of the idea that the claims are directed to—"parsing and encrypting stored data"—*Visual Memory* and *Enfish* show that the claims are not directed to an abstract idea. The patents plainly do not claim every method of parsing data, every method of encrypting data, or every method of both parsing and encrypting stored data. With respect to claim 1 of the '609 patent, for example, the claimed method requires parsing data into chunks, encrypting those chunks with different encryption keys, further encrypting the chunks with another key, and storing each chunk with data indicative of a key on a storage device. This sequence of steps excludes many methods of "parsing and encrypting stored data." For example, parsing data into chunks, encrypting those chunks with a *single* key, and then storing those chunks on one or more storage devices does not appear to be covered by the claims. Parsing data into chunks, encrypting those chunks with number of different keys, storing the chunks in one place, and storing the data indicative of the keys in another place does not appear to be covered by the claims.

One can easily imagine other ways to parse and encrypt stored data that are outside the bounds of the claims.

The asserted claims of the other asserted patents are even further removed from claiming "all types and all forms" of "parsing and encrypting stored data." *Visual Memory*, 867 F.3d at 1259. Whereas claim 1 of the '609 patent is merely permissive of multiple storage devices, the '854, '116, and '140 patents all appear to require the chunks of data (or, in the case of the '140 patent, "shares" of data) to be stored on more than one storage device. '854 patent, claim 1 ("a plurality of different storage devices"); '116 patent, claim 1 (same); '140 patent, claim 1 ("[a] plurality of physical storage devices"). Thus, any method of "parsing and encrypting stored data" that only uses one storage device would appear to be outside the scope of the asserted claims of these patents. Claim 1 of the '140 patent includes additional limitations featuring a "virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device." '140 patent, claim 1. Thus, any method of "parsing and encrypting stored data" that does not utilize the claimed virtual disk is outside the scope of the claim.

Because the asserted claims do not purport to claim "all types and all forms" of "parsing and encrypting stored data," *Visual Memory* and *Enfish* support the proposition that the asserted claims are not directed to that abstract idea.

The panels in *Visual Memory* and *Enfish* also looked to whether the specifications of the asserted patents described any advantages of the claimed invention over the prior art. *See, e.g.*, *Enfish*, 822 F.3d at 1337; *Visual Memory*, 867

F.3d at 1259. Here, the specifications of the asserted patents are, to put it mildly, difficult to navigate. But, at least with respect to the '609 patent, SFI identifies several portions of the specification that describe purported advantages of the claimed invention over the prior art. For example, the specification describes the state of the art and notes that "the foregoing typical public-key cryptographic systems are still highly reliant on the user for security" which means that "the key or keys . . . [are] susceptible to compromise." '609 patent at 1:60–2:3. The invention purports to solve this problem by "provid[ing] cryptographic keys and authentication data in an environment where they are not lost, stolen, or compromised, thereby advantageously avoiding a need to continually reissue and manage new keys and authentication data." *Id.* at 3:21–25. Given that the '854 patent shares the same specification and claim 1 of the '854 patent is substantially similar to claim 1 of the '609 patent, these claimed advantages apply to both patents.

The specification of the '609 patent also describes the advantages of splitting the chunks of parsed, encrypted data onto different storage devices:

> There are major advantages provided by the data security methods and computer systems of the present invention over traditional encryption methods. One advantage is the security gained from moving shares of the data to different locations on one or more data depositories or storage devices, that may be in different logical, physical or geographical locations. When the shares of data are split physically and under the control of different personnel, for example, the possibility of compromising the data is greatly reduced.

'609 patent at 61:33–42. This process of splitting the chunks of data onto more than one storage device is within the scope of claim 1 of the '609 patent ("at least one storage device") and claim 1 of the '854 patent ("a plurality of different storage

devices"), which shares the same specification. Thus, this claimed advantage applies to both patents.

SFI's brief does not identify any purported advantages of the claimed invention that are described in the specifications of the '116 and '140 patents. However, the specifications of these patents reveal essentially the same advantages noted above with respect to the '609 and '854 patents. *See, e.g.*, '116 patent at 1:54–2:7 (describing the problems with prior art approaches), 3:15–22 (describing the advantage of "provid[ing] cryptographic keys and authentication data in an environment where they are not lost, stolen, or compromised"); 3:28–38 (describing the advantage of storing the split data and keys in "multiple depositories"). Thus, as in *Visual Memory* and *Enfish*, the specifications of the asserted patents describe purported advantages of the claimed invention.

Google also argues that the claims are drafted "in highly generic terms" that focus on an "'abstract end-result'" rather than "'a specific means or method for improving technology.'" ECF No. 38 at 15 (quoting *RecogniCorp, LLC v. Nintendo Co., Ltd.*, 855 F.3d 1322, 1326 (Fed. Cir. 2017)). Further, Google submits that the claims provide "no details explaining *how to* implement the claimed software functions." *Id.* at 15–16 (emphasis in original). In support, Google cites *Universal Secure Registry*, asserting that while the patents in that case "sound[ed] in technology," the "individual steps of the limitations, including encryption, were conventional and did not disclose specific means of accomplishing any of the steps." *Id.* at 18.

The claims that were before the Federal Circuit in *Universal Secure Registry* differ significantly from the claims here. The portion of that case Google cites dealt with a claim that was directed to the abstract idea of "multi-factor authentication of a user's identity using two devices to enable a transaction." *Universal Secure Registry*, 908 F.3d at 1354. The court rejected the patentee's argument that "the claims cover an innovative technological solution to address problems specific to prior authentication systems" because, as the court found, "the claims do not include sufficient specificity." *Id.* Specifically, the court found that "[t]here is no description of a specific technical solution by which the biometric information is generated, or by which the authentication information is transmitted." *Id.* at 1355. In other words, the patents in *Universal Secure Registry* failed to explain how the invention accomplished what was purportedly improved about the claimed invention.

Google maintains that the asserted claims are like those in *Universal Secure Registry* because the specification notes that "'any encryption process,'" "'any suitable parsing and splitting algorithm,'" and "any type of data storage and communications" on "'almost any computing device'" can be used to meet the claims. ECF No. 38 at 16–17 (quoting '140 patent at 53:6-9, 6:41-45, 10:8-36) (emphasis removed). Google's argument is beside the point. The "[purportedly] innovative technological solution" of these claims is rooted in the particular sequence of parsing, encrypting, and storing steps they describe, not in any benefits that might flow from the particular method that is used to accomplish each step. Thus, the asserted claims are unlike those in *Universal Secure Registry* because the claims here explain how they implement the

claimed "innovative technological solution." *Universal Secure Registry*, 908 F.3d at 1354.

Google also cites a litany of cases, largely from other district courts, to show that "data encryption (and decryption) is an abstract concept" and that "[g]eneric data handling . . . is also routinely found to be an abstract idea." ECF No. 38 at 17–21. Google's arguments violate the Federal Circuit's instruction not to characterize the claims at "a high level of abstraction" that is "untethered from the claim language." *Enfish*, 822 F.3d at 1337. The claims "require[] more," *TecSec*, 978 F.3d at 1295, than mere "data encryption" and "[g]eneric data handling"—the claims require, e.g., the generation of "data chunks," the encryption of each "data chunk" with a "distinct" encryption key, a "cryptographic operation" with a first key that further secures the data chunks, and the storage of the data chunks with "data indicative" of the distinct encryption keys. '609 patent, claim 1. "[D]isregard[ing] those express claim elements" would be error because those elements form "'the focus of the claimed advance over the prior art.'" *See TecSec*, 978 F.3d at 1295 (quoting *Solutran, Inc. v. Elavon, Inc.*, 931 F.3d 1161, 1167–68 (Fed. Cir. 2019)).

Both Google and SFI filed notices of supplemental authority directing the Court to recent cases from this District that have dealt with questions of abstractness under *Alice*: *Geoscope Techs. Pte. Ltd v. Google LLC*, No. 1:22-cv-1331, 2023 WL 6120603 (E.D. Va. Sept. 18, 2023) and *Daedalus Blue, LLC v. Microstrategy Inc.*, No. 2:20-cv-551, 2023 WL 6221774 (E.D. Va. Sept. 25, 2023).[19] In *Geoscope*, the Honorable

[19] The court's ruling in *Geoscope* is currently on appeal.

Michael S. Nachmanoff held that the asserted patents were invalid under *Alice* because they were directed to "the abstract idea of determining location based on data," *Geoscope*, 2023 WL 6120603 at *5, and "the abstract idea of determining an unknown location by comparing information about known locations organized in a database against measurements from a mobile device," *id.* at *10. In *Daedalus Blue*, the Honorable Roderick C. Young held that the asserted patents were not invalid under *Alice*, finding at step one that the claims disclosed "unique data structures and techniques aimed at solving issues with existing computing systems" and were thus, under *Enfish* and other cases, directed to specific improvements in the way computers operate. *Daedalus Blue*, 2023 WL 6221774, at *17–21.

Geoscope does not persuade the Court that the asserted claims here are directed to an abstract idea. One of the asserted claims in *Geoscope* reads as follows:

> A method for determining a location of a mobile station, comprising:
>
> providing a database of previously-gathered calibration data for a predetermined region in a wireless network;
>
> collecting observed network measurement data, the observed network measurement data collected by the mobile station and transmitted to the network or collected by the network;
>
> modifying said observed network measurement data; and
>
> comparing said modified network measurement data with said database of calibration data to thereby determine the location of the mobile station.

Geoscope, 2023 WL 6120603 at *4 (quoting '494 patent, claim 1). This claim plainly differs substantially from the claims before this Court. Most significantly, this claim

is "both broad and generic"—it essentially captures the entire idea of "determining location based on data," which "has been performed by humans throughout history." *Id.* at *5–6.

As the Court explained above, the asserted claims here do not capture the entire idea of "parsing and encrypting stored data," as Google insists. Rather, with a series of specific sequenced steps, these claims purport to solve a problem that is unique to computers with a solution that only makes sense in the context of computers. The Court's finding at step one is thus consistent with *Daedalus Blue*. *See, e.g.*, *Daedalus Blue*, 2023 WL 6221774, at *20 (finding that the claims and specification of one of the asserted patents identified non-abstract "improvements to computer functionality itself") (quoting *Enfish*, 822 F.3d at 1336) (alteration accepted).

For the foregoing reasons, at *Alice* step one, the Court finds that the claims of the asserted patents are not drawn to an abstract idea. Rather, the asserted claims are directed to a non-abstract improvement in the function of computers: an improved method for securely storing parsed and encrypted data on at least one storage device.

b. Alice *Step Two*

Even if the Court had found at *Alice* step one that the asserted claims are directed to an abstract idea, Google's motion would fail at *Alice* step two. At this step, the Court must ask whether the claims contain an "inventive concept" that transforms the abstract idea into a patent-eligible invention. *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349 (Fed. Cir. 2016). "[T]he search for an 'inventive concept' can also be thought of as a search for a 'limiting concept'—

something that restricts the scope of the claims, ensuring that the patent does not cover the entirety of the abstract idea." *Netflix, Inc. v. Rovi Corp.*, 114 F. Supp. 3d 927, 937 (N.D. Cal. 2015), *aff'd*, 670 F. App'x 704 (Fed. Cir. 2016).

Because the instant motion is a motion to dismiss, there are several statements in the amended complaint that are relevant to *Alice* step two that the Court must accept as true. For example, the amended complaint asserts that the basic steps described by the asserted claims (i.e., "split[ting] the data into multiple portions (e.g., generating a plurality of data chunks based on the data set), encrypting the parsed data (data chunks) using distinct encryption keys, encrypting the distinct encryption keys using an external key, and storing the encrypted, parsed data with data indicative of at least one of the distinct encryption keys on different storage devices") "were unconventional and non-generic, particularly in the context of large scale, server-based data storage." ECF No. 75-1 ¶ 22.

The amended complaint also states that "[t]he idea of securing a data set using encryption after the data set has been split into multiple portions or chunks, as is described in the Asserted Patents, would have been regarded as wholly unconventional at the time of the inventions." *Id.* ¶ 23. It explains that this is so because "performing the encryption/decryption operations on the individual portions that were formed when the original data set was split requires substantial additional processing over what would have been needed to simply encrypt the original single data set." *Id.*

The amended complaint avers that "prior to the Asserted Patents it was unconventional to store 'data indicative of at least one of the distinct encryption keys' with the 'plurality of data chunks.'" *Id.* ¶ 25. This "would have been regarded as creating an insecurity by co-locating encrypted data with information which might facilitate decrypting such data." *Id.*

The amended complaint further asserts that it would have been "unconventional to distribute the split data and the data indicative of the encryption keys across multiple different storage devices." *Id.* ¶ 26. It explains that "[t]his would have required developing an additional mechanism to locate the split data portions across the different storage devices, and then reassembling the different storage devices (after decryption) in order to reconstitute the original data set." *Id.*

In each case, the amended complaint pleads facts and explains why certain features of the asserted claims would have been viewed as unconventional. In addition, each of the alleged inventive features is present in one or more claims. *Cf.*, *e.g.*, *Ericsson*, 955 F.3d at 1328 (finding a patent ineligible at *Alice* step two and noting that that "this allegedly novel aspect of the invention is wholly missing from" the asserted claims). Because SFI has made "plausible and specific factual allegations that aspects of the claims are inventive," *Cellspin*, 927 F.3d at 1317, the Court cannot conclude at this stage "that the claimed elements were well-understood, routine, or conventional," *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1129 (Fed. Cir. 2018); *Cellspin*, 927 F.3d at 1317 ("[P]lausible and specific factual

allegations [in a complaint] that aspects of the claims are inventive are sufficient [to defeat a motion to dismiss.]").

As a result, even if the Court had found at *Alice* step one that the claims are directed to an abstract idea, Google's motion must fail at *Alice* step two.

IV. CONCLUSION

For the foregoing reasons, Plaintiff Security First Innovations, LLC's Motion for Leave to Amend its Complaint (ECF No. 73) is **GRANTED.** SFI may proceed with its claim of willful infringement as to the '140 patent but not as to the remaining asserted patents.[20]

The Clerk is **DIRECTED** to docket ECF No. 75-1 as an amended complaint.

Google LLC's Motion to Dismiss the Complaint (ECF No. 37) is **DENIED.**

Google LLC is **DIRECTED** to respond to the amended complaint within the timeframe prescribed by Fed. R. Civ. P. 12(a)(4).

The Clerk is **FURTHER DIRECTED** to forward a copy of this Memorandum Opinion and Order to all counsel of record.

IT IS SO ORDERED.

/s/
Jamar K. Walker
United States District Judge

Norfolk, Virginia
November 15, 2023

[20] *See, e.g.*, *Diversey, Inc. v. Pops Techs.*, LLC, No. 1:18-cv-04210, 2019 WL 11003292, at *1 (N.D. Ga. Nov. 13, 2019) (granting motion for leave to amend a complaint to add claims for induced and contributory infringement as to one patent but not another).